## CHAPTER 4 –INFORMATION TECHNOLOGY

## ARTICLE 38 — ELECTRONIC MAIL

*Effective July 1, 2013*

### 47110.1 Policy

The California Department of Corrections and Rehabilitation (CDCR) maintains an e-mail system to facilitate business communications and assist employees in performing their daily work activities. This policy outlines the approved use of CDCR e-mail and does not supersede state or federal laws or any other agency policies regarding confidentiality, information dissemination, or standards of conduct.

- The State reserves the right to monitor and/or keep a record of all e-mail communications without prior notice;
- Employees should have no expectation of privacy in the use of CDCR e-mail systems or in anything they store, send or receive on the CDCR's e-mail system.
- The contents of e-mails properly obtained for discovery or management purposes may be disclosed without the permission of the user who created the message.
- E-mail shall be treated as business records that shall be retained and can be used as evidence in litigation, audits, and investigations.
- E-mail may be subject to various types of access requests, including, but not limited to, requests for records under California Government Code (GC) section 6250 et seq.

High Risk Confidential Information (HRCI) shall not be transmitted using e-mail without CDCR approved encryption being applied. Any exclusions or modification to this requirement must be approved in writing by the Information Owner and/or the Information Security Office (ISO).

### 47110.2 Purpose

It is the goal of the CDCR to ensure e-mail communications are being created, maintained and retained consistent with CDCR policy and state and federal laws. The purpose of this policy is to detail the standards relating to the use of e-mail on the CDCR network and is intended to:

- Protect CDCR information;
- Describe privacy considerations when using the CDCR e-mail system;
- Outline the acceptable usage rules when using the CDCR e-mail system;
- Maintain availability of the CDCR e-mail system to sustain critical business operations.

Proper e-mail usage and security is a team effort involving the participation and support of every CDCR employee. It is the responsibility of every computer user to know these guidelines, and to conduct his/her activities accordingly.

This document is not all-inclusive, and the ISO has the authority and discretion to appropriately address any unacceptable behavior and/or practice not specifically mentioned herein.

### 47110.3 Scope
This policy covers appropriate use and retention of the CDCR provided e-mail and applies to all employees, vendors, volunteers, and agents operating on behalf of the CDCR.

### 47110.4 Access to E-mail
CDCR staff may be provided an ID for access to e-mail on the CDCR Network. All access to e-mail shall be protected by password, and all policies pertaining to the use and protection of passwords shall apply. No generic or group access to an ID shall be used. A "group mailbox" is acceptable as long as each individual in the group has his/her own ID and password. If you require someone in addition to yourself to access or monitor your e-mail, establish a rule to forward/copy your mail to another's CDCR mailbox or add them as a delegate. Sharing a password for any reason is prohibited.

### 47110.5 Acceptable Use
The e-mail system is provided for official CDCR business. Using e-mail in an inappropriate manner may result in the loss of e-mail privileges and/or disciplinary action. Examples of appropriate use of the CDCR e-mail system include, but are not limited to, the following:

- Scheduling, coordinating, and documenting business meetings and/or assignments.
- Notifying CDCR personnel of changes in work policies and/or work procedures after the appropriate approval process has been completed (shall be followed up in writing).
- Transmitting and/or sharing non-HRCI work related material, including documents, files, reference material, and links to Internet sites.
- Sending and receiving business related Internet mail.
- Notifying employees of CDCR sanctioned employee events including, but not limited to, the Medal of Honor ceremony, United California State Employees Campaigns, and similar approved activities.
- Scheduling appointments including personal appointments and lunch breaks on an electronic calendar.
- Creating or sending notes or messages of a predominantly personal nature, or for personal use, shall be kept to a minimum.

### 47110.6 Unacceptable Use
Examples include, but are not limited to, the following:

- Using the system to discuss, distribute, or share HRCI without CDCR approved encryption controls.
- Reviewing, receiving, and/or intercepting the electronic communications of another employee without express, advance authorization by the employee or their management.
- Logging on with a user ID and password other than your own.
- Copying or routing notes, messages, documents, or memoranda to individuals who are not involved in the relevant work project or who otherwise have no business related interest in the subject matter of the note, message, document, or memorandum.
- Except as otherwise provided in this policy, reading e-mail of another employee without his/her knowledge and consent.
- Sending sports pool or other forms of gambling messages.
- Using e-mail for any unlawful or illegal endeavor.

- Soliciting or advertising for non-CDCR activities, including fundraising or items of a political nature.
- Allowing access to inmates, wards or parolees, or sending messages on behalf of inmates, wards or parolees.
- Transmitting profanity, obscenity, threatening language, gossip, or derogatory remarks.
- Distributing jokes, poems, chain-letters, or other non-business related material.
- Chain letters and e-mail containing religious, humorous, and political messages are forbidden. E-mail that contains promises, hoaxes, or threats shall not be distributed. Receipt of such e-mail should be reported to management. Forwarding of non-CDCR e-mail is forbidden. It is recognized that recipients cannot control in-coming mail.
- E-mail shall be free of offensive or unlawful material, including slanderous, discriminatory, sexual, pornographic, profane, or revolutionary content. This prohibition applies to e-mail attachments and to the content of Internet sites referenced or linked from e-mail. Displaying, printing, disseminating, or possession of such material may be reason for disciplinary action. The exception to this policy is any material regarding subject matter that may otherwise be considered objectionable that is required for specific work-related purposes may be sent or attached to an e-mail when the material is being sent to a limited number of specified individuals, and not to be sent to group e-mail lists or broadcast statewide.
- Use of the CDCR e-mail system to distribute copyright-protected material such as photographs, graphics, music, documents, etc., without the expressed consent of the copyright holder constitutes a copyright violation, and may result in disciplinary action.

Restrictions on the use of e-mail wallpaper and stationary will be left to the discretion of each Hiring Authority.

### 47110.7 Privacy and Confidentiality

All CDCR e-mail is considered property of CDCR and may be subject to inspection, investigation, Public Records Act (PRA) requests, and/or litigation. Employees, contractors and consultants have no right of privacy with respect to information or messages sent using state-owned equipment and/or resources. E-mail is not private and is subject to monitoring with or without notice.

### 47110.8 Confidential and Sensitive Information

Certain types of information maintained by the CDCR are confidential and protected by state and federal law. The use of e-mail to send confidential information should be limited to an as-needed basis. Never type the information in the body of the e-mail, and never send a password or decryption key in the same e-mail. Unless the file is encrypted or password-protected, it can be read by others and, therefore, is not considered private communication.

Following is a list of the types of information defined as HRCI that shall not be included in e-mail or attached to an e-mail, unless the e-mail and/or attachments are encrypted:

- Personally identifiable information such as a person's name in conjunction with the person's social security number, credit or debit card information, individual financial

account, driver's license number, state ID number, or passport number, or a name in conjunction with biometric information;

- Personal health information such as any information about health status, provisions of health care, or payment for health care information as protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Correctional Offender Record Information as defined in California Penal Code sections 13100-13104;
- Information that if disclosed would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency as specified in GC section 6254.19. Examples include but are not limited to firewall and router configuration information, server names and IP addresses, and other system configuration details;
- Any documentation of information which contains information or data within any Gang Database as defined in the CDCR Department Operations Manual (DOM) sections 52070.22-52070.24;
- Records of investigations, intelligence information, or security procedures as specified in GC section 6254(f); this includes but is not limited to information identifying confidential informants and security procedures contained in DOM section 55000.
- Personnel, medical, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy protected under GC section 6254(c) or the Peace Officers Bill of Rights under GC section 3300 et seq.

Encrypted e-mail must be used when HRCI information is sent to non-CDCR e-mail addresses by placing the keywords of "CDCR Encrypted Message" into the subject line of the e-mail without the quotes. This method should be used only when transmitting HRCI, confidential or sensitive data.

Prior to sending any e-mail, verify the accuracy of the recipient's e-mail address to prevent unintentionally sending it to an unauthorized individual. Once an e-mail is sent outside the department, it cannot be recalled and/or undone.

### 47110.9 Personal Information

Employees shall not seek out or use personal information maintained by the CDCR for their own private interest or advantage. Personal information shall not be transmitted in e-mail or as attachments to e-mail without appropriate encryption controls.

### 47110.10 Unsolicited E-Mail

Unsolicited e-mail may carry viruses. If the sender's identity and intent cannot be verified, such e-mail should be deleted unopened. Unsolicited e-mail from unknown senders should always be deleted unopened. Do not open attachments or Internet links accompanying such unsolicited e- mail.

### 47110.11 Use of Global Distribution Lists

Use of the global distribution list should be limited to departmental, State, or national emergencies, and information from executive levels or program areas that affect all employees.

Distribution of information not required by all employees shall be limited to the affected work groups or physical locations.

### 47110.12 E-Mail Administration

Enterprise Information Systems (EIS) shall perform all administration functions including, but not limited to, establishment of server mailboxes, system-wide filters, and virus scanning functions. EIS shall determine the disk space required to ensure correct functionality of the e-mail system.

### 47110.13 E-Mail Virus Protection

EIS shall manage the virus protection program for all workstations, servers, and network devices. All workstations connected to the CDCR Network or that are Internet accessible shall have the most current Virus Protection software, determined by the EIS. CDCR Network workstations shall be configured to automatically update the virus protection software. Staff shall not disable or turn off this feature. Distribution of virus-laden e-mail may result in performance degradation of the CDCR network and the removal from the network of the workstation(s) from which the infected e-mail is sent.

### 47110.14 Local E-Mail Usage Guidelines

Local operating procedures and guidelines may apply to e-mail content and handling. Local guidelines and procedures are in addition to this e-mail policy and may not be in conflict with or contradictory to this policy.

### 47110.15 Electronic Document Management

The CDCR is committed to ensuring that all departmental electronic documents, including e-mail messages used by staff in the course of their employment, are retained efficiently and in compliance with the Records Management Act, GC section 14740, et seq.

### 47110.16 E-Mail Retention

E-mail messages are official records and are subject to state, federal and CDCR rules and policies for retention and deletion. The E-mail Retention Policy defines how long information sent or received by e-mail should be retained. These policy guidelines cover only information that is either stored or shared via e-mail, including e-mail attachments. This policy establishes retention parameters to effectively capture, manage, and retain e-mail messages. All e-mail (e.g., administrative correspondence, fiscal correspondence, general correspondence) is subject to this policy. This policy applies to all individuals using the CDCR e-mail system. All sent and received e-mail from the department's e-mail system shall be retained for a period of three years.

When litigation is pending or future litigation is reasonably probable, the law imposes a duty upon CDCR to preserve all documents and records that pertain to certain issues. A litigation hold directive overrides any retention policy until the litigation hold has been cleared. E-mail for employees that have been placed on litigation hold must be retained by CDCR until the litigation hold is released or 3 years have passed, whichever occurs later.

### 47110.17 Enforcement

Failure to comply with this policy and associated policies, standards, guidelines, and procedures may result in disciplinary action up to and including dismissal from state service for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal action also may be taken for violations of applicable regulations and laws.

### 47110.18 Deviation from Policy

CDCR staff, contractors, volunteers, and agents operating on behalf of CDCR must comply with all applicable policies rules, standards, procedures and guidelines. Variations and exceptions to this policy will be based on instances where the cost to remediate non-compliant systems exceeds the cost and the risk of remaining non-compliant. Deviations to policy requests are reviewed and analyzed by the ISO, and if the request creates significant risks without compensating controls, it will not be approved.

All approved deviations to policy requests shall have an expiration date and must be reviewed prior to that date to ensure that assumptions or business conditions have not changed, and be reapproved if the deviation policy is still valid.

### 47110.19 Revisions

The Director, EIS, or designee, shall be responsible for ensuring that the contents of this Article are kept current and accurate.

### 47110.20 References

Government Code §§ 6250-6265
California Code of Regulations, Title 15 § 3261.2
California Labor Code § 92
Civil Code, Information Practices Act § 1798
California State Administrative Manual § 5320.5
California Penal Code §§ 13100-13104
California Civil Codes § 17